

RELATÓRIO DO PROJETO

FIREWALL

Disciplina: Sistemas Operacionais

Professor: Clóvis Ferraro

Grupo: 07

Sumário

1. Introdução	3
2. Metodologia.....	3
2.1 Entendendo o Firewall	3
2.2 Sistemas Utilizados.....	4
2.3 Ferramentas utilizadas em cada Sistema	4
2.3.1 Windows Firewall Defender	4
3. Comparação entre os Sistemas Operacionais	5
3.1 Windows Defender	5
3.1.1 Configurações avançadas.	8
3.1.1.1 Incrementando políticas de entrada e saída	8
3.2 Linux.....	14
3.3 Comparação Crítica	19
4. Análise Crítica	19
5. Conclusão.....	20
6. Autoavaliação.....	20
6.1 Dificuldades	20
6.2 Facilidades e conquistas.....	20
7. Referências.....	21

1. Introdução

Este relatório tem como objetivo entender sobre Firewall e sua implementação nos sistemas Windows e Linux. Para entender melhor suas funcionalidades (ajustar)

2. Metodologia

2.1 Entendendo o Firewall

Firewall é uma barreira entre a internet e os computadores, redes locais ou empresariais. Ele pode ser tanto um hardware que como pode ser um software. Que tem sua função de analisar os pacotes de dados com base em regras (políticas) de segurança, impedindo ameaças externas bloqueando, permitindo ou registrando as conexões e os pacotes.

Imagem 1 – Firewall Hardware



Fonte: SupporteSages, 2025

Imagem 2 – Firewall Software



Fonte: Zenarmor, 2025

2.2 Sistemas Utilizados

Para a realização deste relatório será usada a versão do Windows 10 e Linux Ubuntu 24.04.

2.3 Ferramentas utilizadas em cada Sistema

2.3.1 Windows Firewall Defender

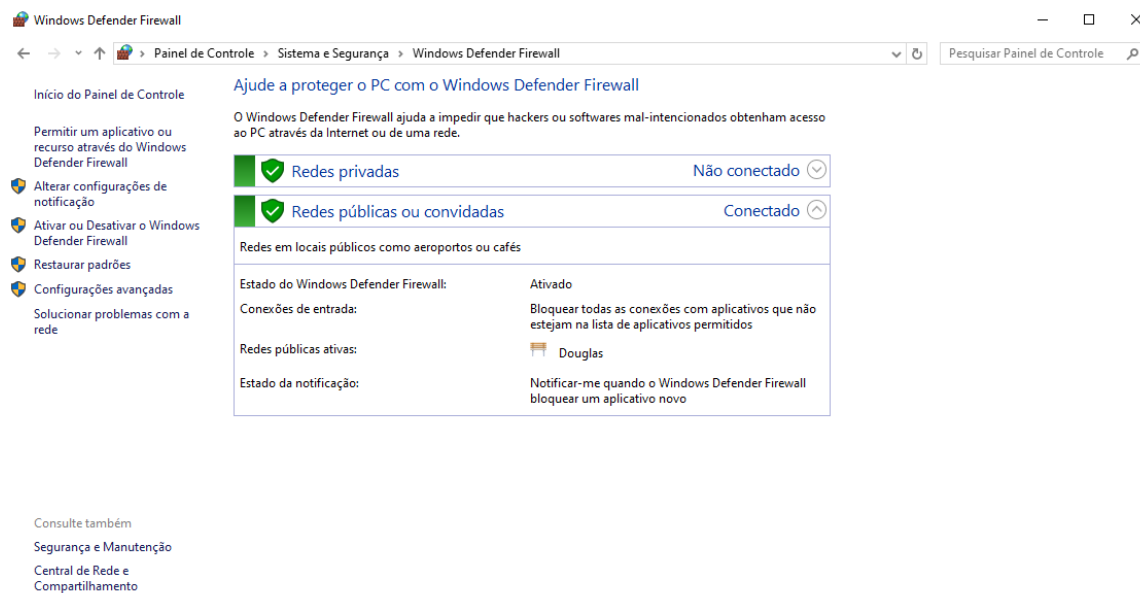
Para acessar o item, basta usar o ícone de pesquisa e pesquisar **Windows Firewall Defender** ou ir em:

Botão Windows + R → Escreva **control panel** → Acesse **Sistema e Segurança**.

3. Comparação entre os Sistemas Operacionais

3.1 Windows Defender

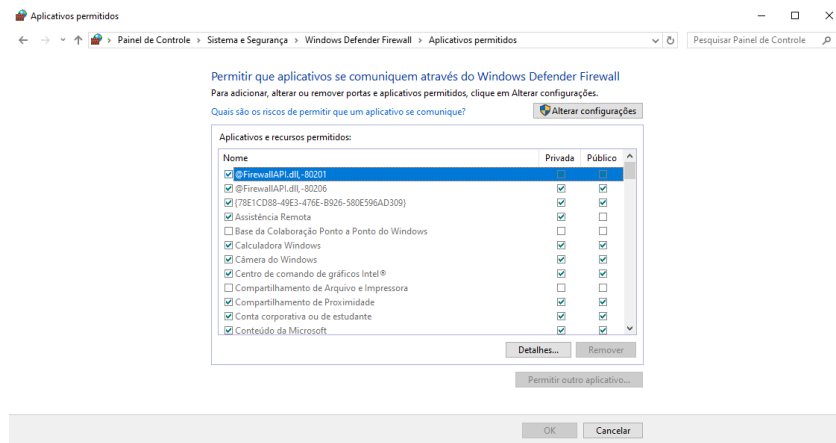
Imagem 3 - Painel principal do Windows Defender



Fonte: Elaborado pelos autores, 2025.

O Windows Defender é simples de mexer, com a sua interface interativa você não precisa ser um gênio dos Firewalls para configurar e proteger seu computador pessoal.

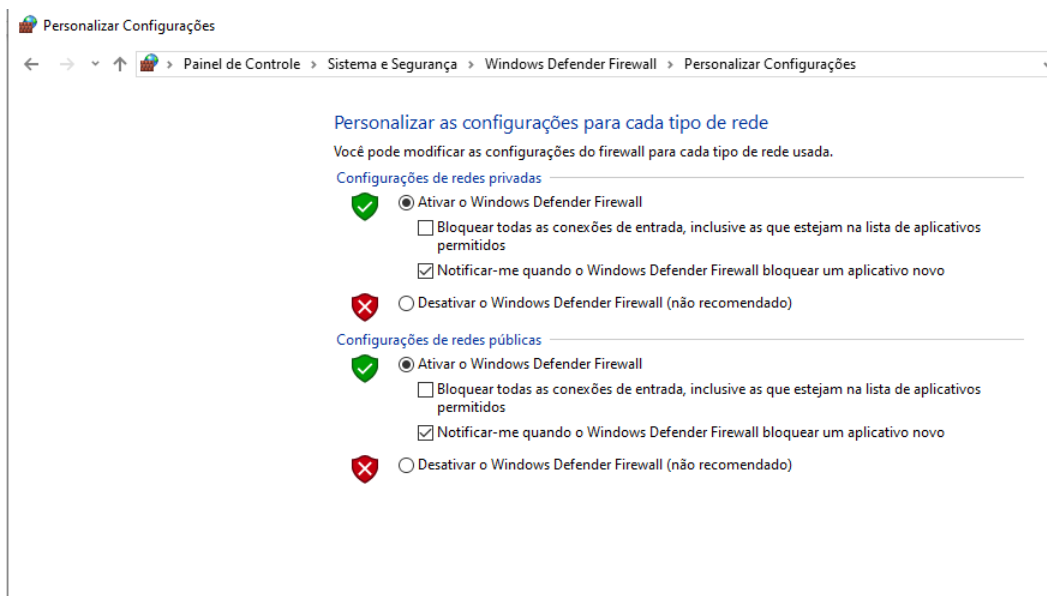
Imagem 4 - Paineis de permissão de aplicativos.



Fonte: Elaborado pelos autores, 2025.

Nessa aba você pode modificar as permissões dos aplicativos para que eles possam se comunicar através da rede. Por padrão ele bloqueia aplicativos que não reconhece garantindo a integridade dos aplicativos.

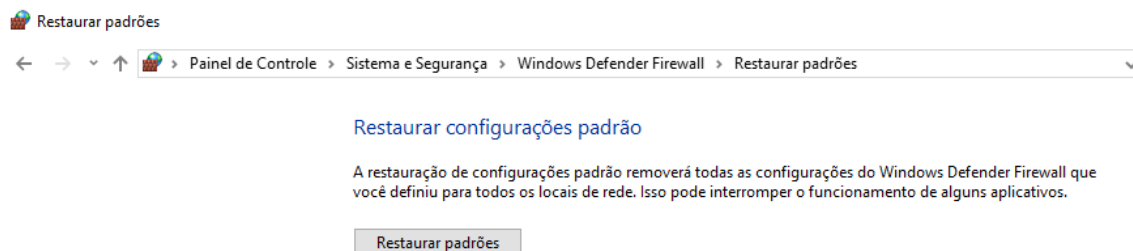
Imagem 5 - Paineis de Notificação.



Fonte: Elaborado pelos autores, 2025.

Painel de notificação serve para alterar as permissões de notificação do Windows Defender, como notificar se ele bloquear algum aplicativo. E traz a opção de desativar o Windows Defender, o que **não é recomendado**.

Imagem 6 – Restaurar padrões.



Fonte: Elaborado pelos autores, 2025.

Caso tenha feito alguma alteração que se arrependa ou não queira mais prosseguir com as configurações e voltar ao padrão de configurações pré-definidas do Windows, pode ser alterado na aba de **restaurar padrões**.

3.1.1 Configurações avançadas.

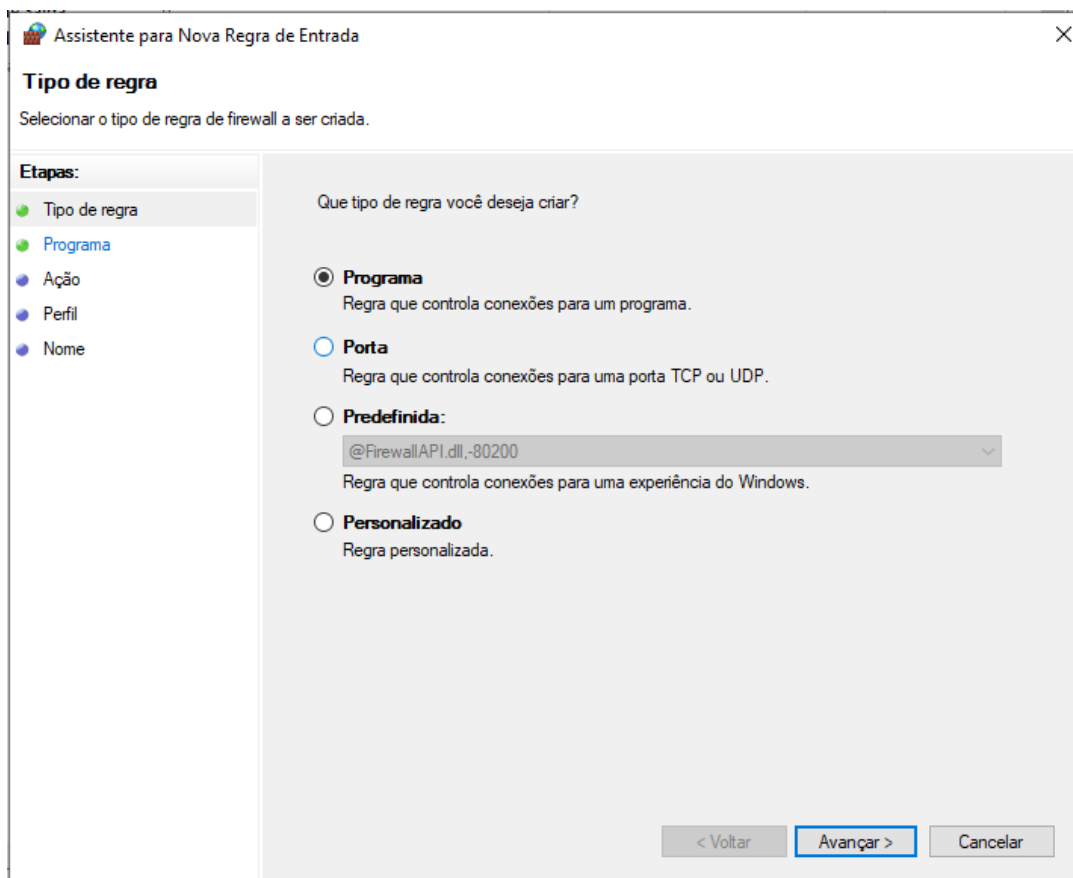
Ao adentrar na área de configurações avançadas é que de fato será incrementado o uso de políticas definidas pelo administrador ou usuário. Podendo impedir qualquer tipo de comunicação de rede.

3.1.1.1 Incrementando políticas de entrada e saída

As regras de firewall controlam o tráfego que entra (entrada) e sai (saída) de uma rede ou sistema, definindo se esse tráfego é permitido ou bloqueado com base em critérios como endereço IP, porta e protocolo. As regras de entrada protegem contra ameaças externas ao bloquear tráfego indesejado, enquanto as regras de saída gerenciam o que pode sair da rede, prevenindo exfiltração de dados ou acesso a sites maliciosos.

Nessa política bloquearemos o Aplicativo Git Hub de fazer conexões de **entrada e saída**.

Imagem 7 – Implementando política.



Fonte: Elaborado pelos autores, 2025.

Imagem 8 – Implementando política.

Programa

Especifique o caminho completo do programa e o nome executável do programa correspondente a esta regra.

Etapas:

Tipo de regra

Programa

Ação

Perfil

Nome

Essa regra se aplica a todos os programas ou a um programa específico?

☐ **Todos os programas**

A regra se aplica a todas as conexões do computador que correspondem às propriedades de outra regra.

☒ **Este caminho de programa:**

Exemplo: c:\path\program.exe
%ProgramFiles%\browser\browser.exe

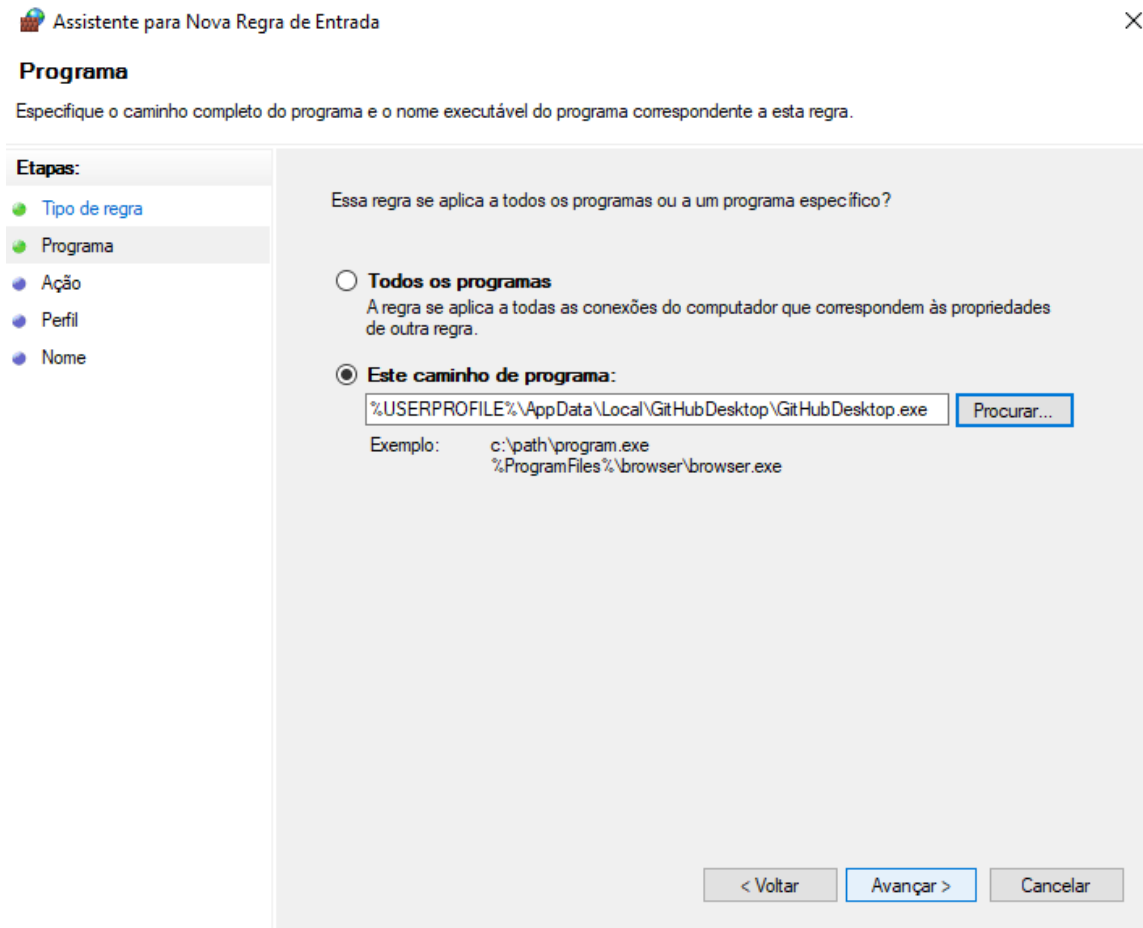
< Voltar

Avançar >

Cancelar

Fonte: Elaborado pelos autores, 2025.

Imagem 9 – Implementando política.



Fonte: Elaborado pelos autores, 2025.

Imagem 10 - Implementando política.

Assistente para Nova Regra de Entrada

Ação

Especifique a ação executada quando uma conexão atender às condições especificadas na regra.

Etapas:

- Tipo de regra
- Programa
- **Ação**
- Perfil
- Nome

Que ação deve ser tomada quando uma conexão corresponde às condições especificadas?

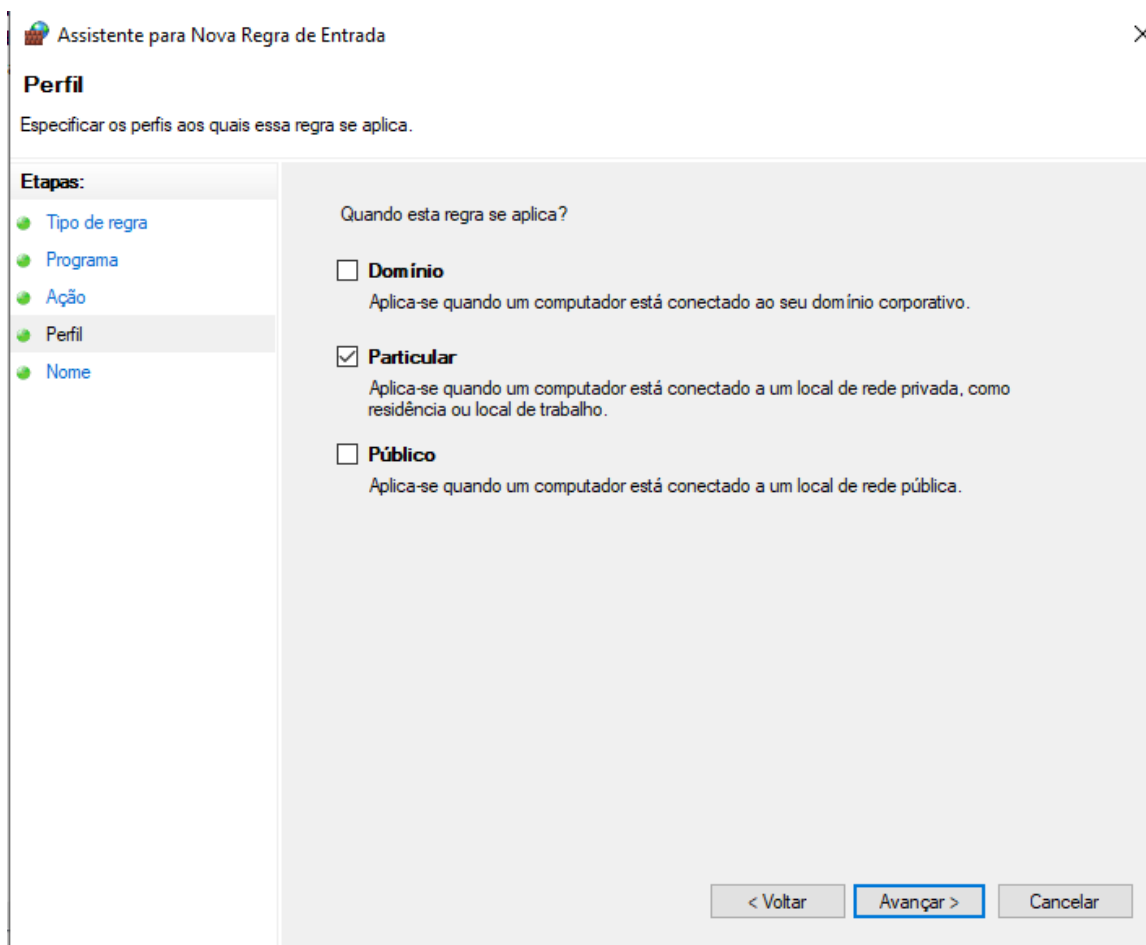
☐ **Permitir a conexão**
Isso inclui conexões protegidas com IPsec bem como as sem essa proteção.

☐ **Permitir a conexão, se for segura**
Isso inclui conexões que foram autenticadas usando IPsec. As conexões serão protegidas por meio de uso das configurações nas regras e propriedades IPsec no nó Regra de Segurança de Conexão.

☒ **Bloquear a conexão**

< Voltar Avançar > Cancelar

Fonte: Elaborado pelos autores, 2025.

Imagem 11 – Implementando política.

Fonte: Elaborado pelos autores, 2025.

Imagem 12 – Implementando política.

Fonte: Elaborado pelos autores, 2025.

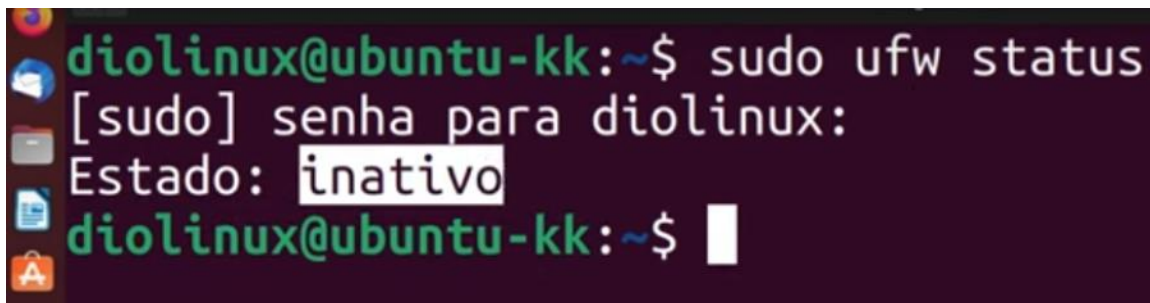
Está política implementada tem o objetivo de impedir a comunicação do aplicativo com a internet. Fazendo assim ficar desconectada mesmo a máquina estando conectada.

3.2 Linux

Ferramentas: UFW (Uncomplicated Firewall). O UFW permite que as configurações sejam feitas de uma forma mais simples, apresenta uma interface gráfica (GUFW) que pode ser instalado em qualquer sistema, facilitando ainda mais o funcionamento para o usuário.

Procedimentos: Na distribuição Ubuntu o UFW já vem pré-instalado, porém desligado. Para fazer essa verificação é necessário o uso do comando `sudo ufw status` no terminal, e mostrar status inativo.

Imagem 13 – Implementando políticas pelo Linux Ubuntu.

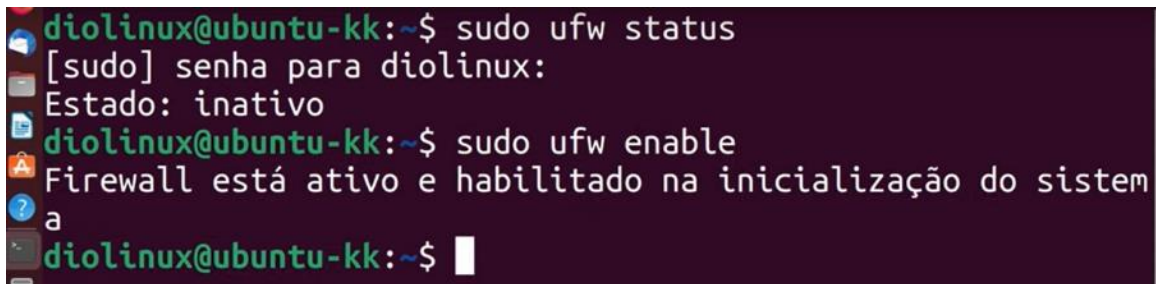
A terminal window with a dark purple background and green text. The prompt is 'diolinux@ubuntu-kk:~\$'. The command 'sudo ufw status' has been entered. The output shows '[sudo] senha para diolinux:' followed by a password input field (represented by dots). Below that, it says 'Estado: inativo'. The prompt returns to 'diolinux@ubuntu-kk:~\$' with a cursor at the end.

```
diolinux@ubuntu-kk:~$ sudo ufw status
[sudo] senha para diolinux:
Estado: inativo
diolinux@ubuntu-kk:~$
```

Fonte: Elaborado pelos autores, 2025.

Para ativar ou desativar o UFW a gente usa o comando **sudo ufw enable** para ativar e **sudo ufw disable** para desativar.

Imagem 14 – Implementando políticas pelo Linux Ubuntu.

A terminal window with a dark purple background. The prompt is 'diolinux@ubuntu-kk:~\$'. The first command is 'sudo ufw status', followed by a password prompt '[sudo] senha para diolinux:' and the output 'Estado: inativo'. The second command is 'sudo ufw enable', followed by the output 'Firewall está ativo e habilitado na inicialização do sistema'. The prompt returns to 'diolinux@ubuntu-kk:~\$' with a cursor.

```
diolinux@ubuntu-kk:~$ sudo ufw status
[sudo] senha para diolinux:
Estado: inativo
diolinux@ubuntu-kk:~$ sudo ufw enable
Firewall está ativo e habilitado na inicialização do sistema
diolinux@ubuntu-kk:~$
```

Fonte: Elaborado pelos autores, 2025.

Por padrão, o UFW é habilitado como:

- Negar todas as conexões de entrada.
- Permitir todas as conexões de saída.

Pode-se verificar as configurações de política padrão atuais com o comando:

Imagem 15 – Implementando políticas pelo Linux Ubuntu.

Two terminal window screenshots. The top one shows the command '\$ sudo ufw status verbose' in a dark blue terminal. The bottom one shows the output of the command in a dark blue terminal with a 'Saída' header.

```
$ sudo ufw status verbose
```

Saída

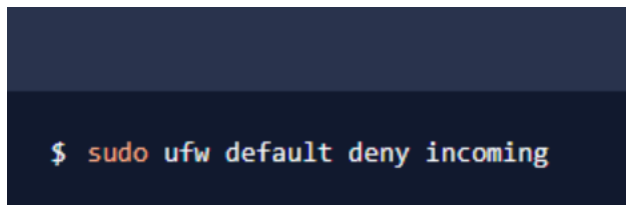
```
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), deny (routed)
New profiles: skip
```

Fonte: Elaborado pelos autores, 2025.

Caso queira alterar o comportamento padrão, pode-se atualizar as políticas padrão com os comandos:

-Para negar todas as conexões de entrada:

Imagem 16 – Implementando políticas pelo Linux Ubuntu.

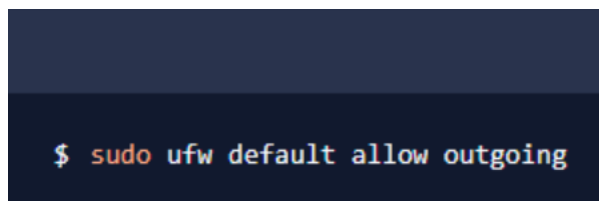
A terminal window with a dark background. The prompt is a dollar sign '\$'. The command entered is 'sudo ufw default deny incoming' in a light blue monospace font.

```
$ sudo ufw default deny incoming
```

Fonte: Elaborado pelos autores, 2025.

-Para permitir todas as conexões de saída:

Imagem 17 – Implementando políticas pelo Linux Ubuntu.

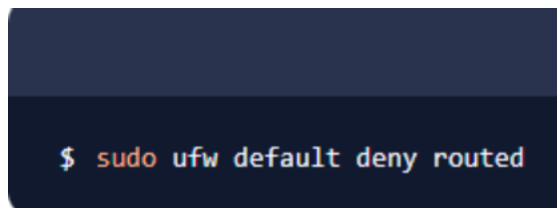
A terminal window with a dark background. The prompt is a dollar sign '\$'. The command entered is 'sudo ufw default allow outgoing' in a light blue monospace font.

```
$ sudo ufw default allow outgoing
```

Fonte: Elaborado pelos autores, 2025.

-Para negar todo o tráfego encaminhado:

Imagem 18 – Implementando políticas pelo Linux Ubuntu.

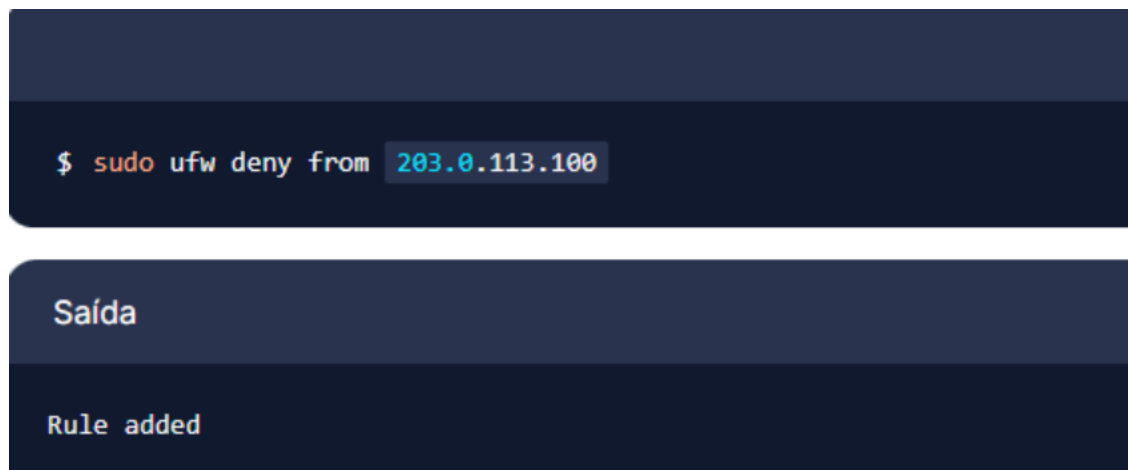
A terminal window with a dark background. The prompt is a dollar sign '\$'. The command entered is 'sudo ufw default deny routed' in a light blue monospace font.

```
$ sudo ufw default deny routed
```

Fonte: Elaborado pelos autores, 2025.

Para impedir todas as conexões de rede vinda de um endereço IP em particular, utilize o comando abaixo, substituindo o IP em destaque pelo endereço que deseja bloquear.

Imagem 19 – Implementando políticas pelo Linux Ubuntu



Fonte: Elaborado pelos autores, 2025.

Ao rodar o comando **sudo ufw status** neste momento, você verá que o endereço IP indicado aparece como bloqueado.

Imagem 18 – Implementando políticas pelo Linux Ubuntu.



Fonte: Elaborado pelos autores, 2025.

Análise dos comandos:

O UFW é conhecido por ter uma interface acessível e por ser mais simples. Ele facilita a administração de regras por meio de comandos objetivos, sendo uma boa escolha para quem prioriza praticidade. Já o IPTABLES utiliza sintaxe mais elaboradas, permitindo um controle mais detalhado, porém exige maior conhecimento técnico.

Após comparar UFW e IPTABLES, podemos concluir que: UFW é indicado quando a prioridade é simplicidade, já o IPTABLES atende melhor a sistemas antigos com regras complexas.

3.3 Comparação Crítica

Com os resultados obtidos pode-se verificar uma facilidade maior e interatividade com o uso do Windows, pois como sua proposta é ser mais fácil aos usuários acaba que é mais confortável e organizado de criar políticas. Enquanto o Linux é na base do CLI que apesar de ser um pouco mais complicado é muito interessante ver o desenvolvimento e criação de uma política por meio de linhas de comando.

4. Análise Crítica

O Sistema Windows se mostra superior em questão de design e facilidade a usuários mais simples, que querem implementar políticas simples/básicas.

O Linux já se mostra complicado pelo fato de ser por comandos, mas nada que testando e aprendendo que não seja possível de fazer.

5. Conclusão

Com os resultados obtidos pode-se entender que o Firewall atua na rede como uma barreira impedindo o acesso a internet ou a entrada e saída de pacotes maliciosos ou prejudiciais a redes ou computadores. E sua implementação em sistemas operacionais diferentes com o bloqueio de entrada e saída de um app para a internet como o bloqueio da rede em uma máquina. Vale ressaltar que esses resultados podem ser diferentes em outros sistemas operacionais.

6. Autoavaliação

O grupo se mostrou unido e colaborativo na realização deste projeto, sendo assim todos podemos ver a implementação e utilização de políticas por meio do uso dos Firewall's citados. Abaixo terá pontos que foram observados ao longo do processo.

6.1 Dificuldades

Para entender o uso do Windows Defender tivemos que realizar pesquisas e utilizar da máquina própria.

O Linux se mostrou mais difícil por ser linha de Código e tivemos que traduzir o que cada Código estava fazendo.

6.2 Facilidades e conquistas

Apesar das dificuldades foi muito divertido ver o grupo disposto e melhor ver como ocorre o uso de políticas por meio da rede.

7. Referências

YOUTUBE. *Firewall explicado de forma simples*. Disponível em: <https://www.youtube.com/watch?v=0W7y0QxVIEY>. Acesso em: 27 set. 2025.

YOUTUBE. *Você já deveria saber configurar um Firewall! - Linux UFW e GFW*. Disponível em: <https://www.youtube.com/watch?v=BZ4yuTQmxdo>. Acesso em: 27 set. 2025.

GOOGLE CLOUD. *Firewall policy rule details*. Disponível em: <https://cloud.google.com/firewall/docs/firewall-policies-rule-details?hl=pt-br>. Acesso em: 27 set. 2025.

DIGITALOCEAN. *UFW essentials: common firewall rules and commands*. Disponível em: <https://www.digitalocean.com/community/tutorials/uw-essentials-common-firewall-rules-and-commands>. Acesso em: 27 set. 2025.

BAELDUNG. *Difference Between UFW vs. nftables vs. iptables*. Disponível em: <https://www.baeldung.com/linux/uw-nftables-iptables-comparison>. Acesso em: 27 set. 2025.